Safety and Mission Assurance Plan

Checkout and Launch Control System (CLCS)

84K00055

(K-EC-0001.23)

Approval:

Project Manager, CLCS Date

Chief, System Engr. & Integ. Date

CLCS Project Controls Office Date

CHECKOUT AND LAUNCH CONTROL SYSTEM (CLCS) PROJECT SAFETY AND MISSION ASSURANCE (S&MA) PLAN

PREFACE

This plan describes the S&MA (safety, reliability, maintainability and quality assurance) support to the CLCS Project, which is to replace the current Launch Processing System with state-of-the art technology.

This plan applies to the KSC organizations and contractor organizations, as provided in the provisions of their respective contracts, providing personnel to support this project.

This plan establishes the policies and procedures for accomplishing the S&MA tasks as an integral part of the project effort. It provides for early implementation of S&MA tasks during development. The requirements in this plan shall be carefully and conscientiously documented, implemented and tracked to ensure total project support.

The CLCS Project S&MA Working Group developed the plan, any questions regarding it should be directed to the working group lead, Independent Assessment and Project Office, EC-E.

This plan is a new issuance.

original signed by
P. Thomas Breakfield, III
Director of Safety and
Mission Assurance

PREPARED BY:

REVISION HISTORY

REV	DESCRIPTION	DATE

LIST OF EFFECTIVE PAGES

Dates of issue of change pages are:

Page No.	**A or D***	**Issue or Change No.**	**CR No.**	**Effective Date****
	Initial	Basic		April 28, 1997

TABLE OF CONTENTS

PAR. Page

SECTION 1: INTRODUCTION

SECTION 2: SAFETY, RELIABILITY AND MAINTAINABILITY

SECTION 3: QUALITY ASSURANCE

SECTION 1: Introduction

100 MANAGEMENT AND ORGANIZATION OF THE CLCS PROJECT S&MA PROGRAM

1. The CLCS Project S&MA Working Group shall implement the requirements listed in this plan. The support shall be provided early in the project to ensure complete integration of effort, and shall be provided for all hardware and software procured or developed for the CLCS. The S&MA Working Group shall integrate its efforts to assure that these assurance functions are adequately provided with no duplication of effort.

2. These functions shall be in compliance with NSTS 07700 Volume X, NHB 5300.4(1D-2), ANSI/ASQC Q9001, and other project required documents.

3. The S&MA Working Group lead reports to the CLCS Project Manager through the Systems Engineering and Technical Integration Manager.

101 SAFETY AND MISSION ASSURANCE ACTIVITIES

1. *Safety, Reliability and Maintainability.* The safety and reliability analyses will be performed to identify the risks associated with hazards or critical items in the CLCS system. Maintainability design criteria will be provided to support the ease of maintenance, fault isolation and detection, etc. These analyses shall be applied throughout all phases of the life cycle, starting in the design phase, and maintained to assure a continual methodology exists for the reduction or elimination of potential risks.

2. *Quality Assurance.* Quality Assurance will be performed to provide adequate confidence that the CLCS Project conforms to the project requirements

3. *Software Product Assurance.* The Software Product Assurance Program is to assure the quality of all software and its documentation, and assure the quality of the processes used to produce software. Where possible, software product assurance activities

will be accomplished on a non-interference basis (insight) using surveillance techniques and be applied in conjunction with the S&MA activities.

102 PROJECT SUPPORT

1. *S&MA Support.* CLCS is a NASA managed re-engineering activity with contractor support provided under the existing NASA contracts. S&MA support will be provided to the project by the Safety and Mission Assurance Directorate (EC). EC will provide the S&MA management with the contractors implementing support in accordance with the provisions of their respective contracts.

2. S&MA Personnel shall:

   a. Evaluate and assess CLCS design to ensure safety, reliability, maintainability and quality assurance aspects are recognized and optimized with due consideration to costs, benefits, and availability of resources.

   b. Provide safety, reliability, and maintainability design criteria for the CLCS Design. CLCS design shall incorporate, as a minimum, the following features.

      (1) Fail-safe philosophy.

      (2) Minimum Hazards.

      (3) Simplicity.

      (4) Component (line-replaceable unit (LRU) accessibility.

      (5) Component (LRU) replaceability.

      (6) Serviceability.

      (7) Identification of limited-life parts.

      (8) Failure propagation safeguards.

   c. Interact with design, system engineers, and maintenance personnel during all design phases ensuring adequate safety, reliability, maintainability and quality assurance requirements enhance CLCS inherent availability goal.

d. Participate in design reviews to ensure no new critical items or hazards are introduced, nor degradation of established controls for existing critical items or hazards has occurred.

e. Participate in design trade studies and product evaluations to assess safety, reliability and maintainability requirements for each design, utilizing numerical modeling as appropriate.

103 APPLICABLE REFERENCE DOCUMENTS

1. NHB 5300.4(1D-2), “Safety, Reliability, Maintainability and Quality Assurance Provisions for the Space Shuttle Program”

2. NSTS 07700, Volume X, “Space Shuttle Flight and Ground Systems Specifications”

3. KHB 1710.2, “KSC Safety Practices Handbook”

4. KHB 5330.9, “Metrology and Calibration Handbook”

5. ANSI/ASQC Q9000-1994, “Quality Systems - Model for Quality Assurance in Design, Development, Production, Installation and Servicing”

6. NSTS 22254, “Methodology of Conduct of Hazard Analyses”

7. NSTS 22206, “Requirements for Preparation and Approval of Failure Modes and Effects Analyses (FMEA) and Critical Items List (CIL)”

8. NSS 1740.13, “Software Safety Standard”

9. NASA-STD-2201-93, Software Assurance Standard”

SECTION 2: SAFETY, RELIABILITY AND MAINTAINABILITY

200 SAFETY, RELIABILITY AND MAINTAINABILITY

201 SYSTEM ASSURANCE ANALYSES

The System Assurance Analysis is the document that combines the Safety and Reliability analysis, and any other applicable analysis into one report for the CLCS system. The analysis is to determine if the system can be safely operated.

1. Safety Analysis. The safety analysis determines the design operational hazards utilizing Hazard Analysis, Fault Tree Analysis and Safety Assessments.

2. Criticality Assessment. The criticality assessment is an analysis of system functions to determine if loss or improper performance of the function could result in loss of life and/or vehicle or damage to a vehicle system.

3. Reliability Analysis. The reliability analysis identifies critical items utilizing Failure Mode and Effects Analysis (FMEA) and Fault Tree Analysis (FTA) as appropriate.

4. Software Safety Assurance. Software Safety Assurance is concerned with the satisfaction of system safety requirements that are allocated to the software, and the identification and verification of adequate safety controls and inhibits that are to be implemented in software.

5. Trade Studies. Trade studies are not part of the System Assurance Analyses (SAA), however, the SAA FMEA, along with data obtained from the Vendors (MTBF, MTTR, etc.) will provide valuable information for the trade study solution.

202 PROJECT SUPPORT DETAILS

S&MA Personnel shall:

1. Perform safety and reliability analysis as an integral part of the design process to aid CLCS

design engineering in the elimination of critical items/hazards or to develop rationale for acceptance of the risk associated with the use of the CLCS system with critical items/hazards.

2. Perform a Criticality Assessment of CLCS functions to determine the impacts encountered if the function is performed incorrectly or not at all.

3. Perform a failure mode and effects analysis (FMEA) and hazard analysis on CLCS functions identified as critical in the Criticality Assessment.

4. Prepare and process critical items through the appropriate risk reviews, for those critical items not eliminated by design.

5. Prepare a Hazard Report for those hazards not eliminated by design.

203 SOFTWARE SAFETY

The following activities shall be performed as part of the software safety assurance program. This program shall meet the intent of NSS 1740.13.

1. Ensure the identification of safety-critical software.

2. Identify and ensure incorporation of safety requirements in system requirements specification and subsequent design documentation.

3. Ensure appropriate verification and validation requirements are established.

4. Ensure test plans and procedures adequately test safety requirements and the test results are satisfactory.

204 INDUSTRIAL SAFETY

Industrial Safety activities shall be in compliance with KHB 1710.2 and organizational safety procedures. Industrial Safety includes identification, elimination, and or control of hazards in the work place, accident prevention, fire prevention and protection, and transportation accident prevention.

205 TEST OPERATIONS SAFETY

Test Operations Safety activities shall be in compliance with KHB 1710.2. Test Operations includes procedure reviews, safety monitoring, and providing a margin of safety in test operations.

SECTION 3: QUALITY ASSURANCE

300 QUALITY ASSURANCE

301 MANAGEMENT AND ORGANIZATION OF THE QUALITY PROGRAM

Quality Engineering(QE) shall ensure implementation of all the quality requirements listed in this plan. Support shall be provided early in the project to ensure all quality planning is provided for all hardware and software procured or developed for the CLCS. The QE shall integrate its efforts with other Safety and Mission Assurance (S&MA) functions, such as Safety, Reliability, Maintainability and Software Assurance to assure that these assurance functions are adequately provided with no duplication of effort.

The QE functional support shall be in compliance with NSTS 07700, NHB 5300.4(1D-2), ANSI/ASQC Q9001, and other project requirements.

302 QUALITY PROGRAM AUDITS

In conjunction with the project schedule, QE will provide timely and effective support to program audits of the CLCS. Reports of these audit activities will be forwarded to the S&MA Management and to the CLCS Project Manager, and submitted to the Systems Engineering and Technical Integration Manager for proper disposition.

303 PROJECT SUPPORT DETAILS

QA and QE supports the CLCS Project through all phases of the project. These phases, and associated support, are listed below:

1. *Preliminary Planning/Procurement*

    a. QE shall document and conscientiously track all quality requirements as listed in this plan. As directed by Project management, requirements tracking shall be provided for other aspects of the Project. Tracking shall be implemented with a thorough database program. Requirements will be developed and traced back to this plan, or to other pertinent project documents, and tracked to closure.

b. Procurement Quality Assurance (PQA) shall provide reviews of all purchasing documentation, such as Purchase Requests (PR’s) and other acquisition paperwork. Also, PQA shall review all procurement packages for inclusion of S&MA requirements as necessary. The PQA shall maintain a log and file copy of each PR reviewed, and its disposition. The PQA shall indicate approval by signing the procurement packages reviewed, as directed by project management.

c. PQA and/or QE shall participate in source selection as required.

d. QE and/or PQA shall develop quality requirements. These requirements, which will be developed through closely working with design engineers and other CLCS personnel, are as follows:

(1) Supplier’s change control provisions.

(2) Preservation, packaging, packing and shipping provisions.

(3) Storage requirements.

(4) Age-controlled and life-limited records and controls.

(5) Identification and data retrieval controls.

(6) Inspection and test criteria, including receiving inspection.

(7) Nonconforming material controls.

(8) Government Source Inspection (GSI) requirement provisions.

(9) Provisions for GSI where GSI is not invoked.

(10) Detailed requirements of equipment records.

(11) Electrostatic Discharge (ESD) controls.

(12) Mandatory Inspection Points (MIP)

e. PQA shall provide source inspection, as required.

f. PQA shall provide for audits of suppliers, as required.

g. QA shall ensure material inspection upon receipt of procured items. This inspection includes physical condition, quantity, proper model and serial numbers, inclusion of proper documentation, etc. QA provisions shall be maintained for received items, including the following:

(1) Logging of received items.

(2) Assurance of compliance with Receiving Inspection checklist.

(3) Environmental conditions for storage.

(4) Segregation of received items to ensure that items in various phases of the receiving process are stored separately.

(5) Proper identification of segregated items (tagging, log books, etc.)

(6) Receiving testing. Any testing procedure shall be documented and the procedure approved prior to actual testing.

(7) Assurance that item integrity is maintained in the event of testing. It is imperative that the item not be violated or tampered with intrusively, to maintain the item’s integrity, for personnel safety

2. *Design and Development*

a. QE shall ensure review of applicable submitted vendor and contractor documentation, as well as documentation developed by CLCS personnel. Documentation can include drawings, logic diagrams, Quality Plans, Failure Modes and Effects Analyses (FMEA’s), Software Analyses, Hazard Analyses, etc. Reviews shall ensure compliance with appropriate NASA requirements, and shall be indicated by the reviewer initialing of reviewed documents.

b. QE shall ensure proper handling of all documentation received and generated through inclusion of such documents into the CLCS Configuration Management (CM) system. Documents shall be submitted to CM immediately upon receipt or final signoff, if generated in-house.

c. QE shall provide support during testing phases of CLCS development. This support shall include the following:

(1) Requirements definition resulting from testing shall be carefully documented in a requirements matrix, and tracked and implemented as appropriate.

(2) Review of test plans for S&MA concerns. Careful consideration shall be given to maintaining integrity of test equipment.

(3) Careful consideration shall be given to assuring maintenance of hardware and software, and to inclusion of changes to software/hardware during and as a result of the testing.

(4) Assurance of ability to duplicate tests to verify the integrity of tests.

d. QE shall provide review of processes employed on the CLCS. These processes shall be reviewed for the following:

(1) Documentation of process.

(2) Adherence to documented process by those performing the process.

(3) Configuration management and revision control of documented process, and of other related documentation.

(4) Training of those performing the process.

(5) Utilization of a noncompliance/problem reporting and corrective action system, described below.

e. QE shall provide day to day support to the CLCS. This includes the following:

(1) Timely review of purchase documents, problem reporting documents, analysis, drawings, change orders, and any other requested documents.

(2) Technical support, as directed by the Project Manager and S&MA Manager.

(3) Review of all change requests (CR). A record of each CR reviewed shall be maintained.

(4) Waivers/deviations review. A record of each waiver or disposition shall be maintained.

f. QE shall provide support at all design reviews and readiness reviews, as required in DE-P 450. The status of all S&MA functions shall be given at these reviews.

3. *Testing/Checkout Phase*

a. QE support during the testing and checkout phase shall consist of the following:

(1) Review of all test plans for S&MA concerns and requirements.

(2) Assurance that test results' integrity and security are maintained.

(3) Assurance that tests are documented, verifiable and can be replicated.

(4) As part of S&MA support during this phase, QE shall indicate approval of all documents reviewed via initials, or signature, at the discretion of the Project Manager.

b. QA support during the testing and checkout phase shall consist of the following:

(1) Assurance that actual hardware is not used in testing; rather, prototype or simulated hardware, and conditions are utilized, except where absolutely necessary.

(2) Assurance that all changes to test documents and associated software and hardware are controlled, documented and approved via the change control system.

(3) Assurance that testing equipment is properly calibrated, stored, and controlled.

(4) Assurance that unexpected test results are documented and that their anomalous nature is investigated.

304 NONCONFORMANCE/PROBLEM REPORTING AND CORRECTIVE ACTION

QE shall ensure that the CLCS implements an effective Nonconforming/Problem Reporting And Corrective Action (N/PRACA) system that provides for the following:

1. The documenting, tracking, dispositioning and reporting of all nonconformances found during all phases (development, fabrication, testing, inspections, etc.) of the CLCS Project.

2. Proper and uniform handling of all items received or developed that do not meet requirements,

specifications, drawings, or other controlled project documentation.

3. Provisions to identify, segregate (if possible) and document all nonconforming articles from other items. This step includes tagging, labeling, or some other type of secure labeling system.

4. Review of nonconforming articles to determine their disposition. The nonconforming article will be dispositioned in one of the following categories:

   a. Reworked to meet specified requirements.

   b. Material Review Board accepted with or without repair.

   c. Used for alternative applications on other parts of the Project.

   d. Rejected or scrapped.

   e. Return to supplier.

5. When a nonconformance is to be reworked or modified, QE shall review the project engineers disposition to evaluate the acceptance criteria and procedures for the item. These criteria shall include any restrictions on the use of the reworked nonconformance.

6. When a nonconformance is identified, corrective actions shall be taken to determine the cause(s) of the nonconformance, and to prevent its future recurrence. These actions shall be taken by the appropriate CLCS lead, in conjunction with the QE, for the group or thread that has engineering cognizance for the item. These actions are as follows:

   a. Investigate, review and analyze the nonconformity.

   b. Determine the root cause of the nonconformity. This step may involve visual inspection, document and record review, engineering analysis, etc.

c. Develop or change procedures, drawings, or any other related controlled documents to ensure prevention of the nonconformance.

305 FABRICATION CONTROL

1. QA/QE shall ensure the following:

2. All items fabricated by DE shall be subjected to inspection and/or surveillance to ensure conformance to the document governing its fabrication. Governing documents shall include drawings, logic diagrams, requirements lists, specifications, etc. All governing documents shall be under the CLCS Configuration Management (CM) system, and shall include appropriate revision and control identification. Documents shall not be used for inspection purposes if they are not clearly under the control of the CM system.

3. Adherence to documented procedures through inspections and procedure reviews. Each documented procedure shall include the following:

   a. Title

   b. Purpose

   c. Application

   d. Exact references to other documents, standards, etc.

   e. Materials used in performing the procedure

   f. Equipment/Special Tooling List

   g. Personnel training/certification Requirements

   h. Approvals/Signatures authorizing work

4. Work documents shall include:

   a. General information, including constraints, cautions, warnings, preparations

b. Step by step detailed operations in performing the procedure

c. Maintenance and certification requirements

d. Inspection and test provisions to control the process

e. Material handling and/or storage requirements

f. Environmental, safety and health issues

5. Any nonconformance detected at any time during any process shall be documented.

6. All applicable equipment used or acquired during design, development, fabrication, testing and checkout shall be calibrated in accordance with KHB 5330.9. All calibration equipment shall be traceable back to NIST standards.

306 SOFTWARE QUALITY ASSURANCE

Software Quality Assurance (SQA) will conduct evaluations of the quality of, and adherence to, software-related standards and procedures. The following activities shall be performed, as a minimum, as part of a Quality Surveillance Program, which shall meet the intent of NASA STD-2201-93.

1. Review software requirements for completeness, testability, and that they properly express the functional, performance and interface requirements.

2. Ensure adherence to design standards, and completeness of design.

3. Ensure up-to-date verification/traceability matrix.

4. Ensure adherence to coding and documentation standards.

5. Auditing conformance to procedures, i.e. configuration management, nonconformance reporting, software development library.

6. Ensure test readiness, compliance to test plans and procedures, documentation of nonconformances, complete and correct test reports.

7. SQA is concerned with incorporating reliability, maintainability, usability, and similar requirements into the products produced at each phase of the development life cycle.

8. SQA will evaluate the development process and the conformance to this process through process audits (e.g., nonconformance process, configuration management) and surveillance of activities (e.g., design reviews, code walkthroughs, etc.) performed throughout the development process.

9. Provide and evaluate quality requirements and ensure the product satisfies these requirements.

10. Evaluate nonconformance trends and make recommendations on process improvements.